TITLE: OUT-OF-BAND SECURITY NETWORKS FOR COMPUTER NETWORK APPLICATIONS

BACKGROUND OF THE INVENTION

1. Field of the Invention.

This invention relates to security networks for computer network applications, and, more particularly, to a security network which provides user authentication by an out-of-band system that is entirely outside the host computer network being accessed. In addition, the out-of-band system optionally includes provision for biometric identification as part of the authentication process.

2. Background of the Invention.

In the past, there have typically been three categories of computer security systems, namely, access control, encryption and message authentication, and intrusion detection. The access control systems act as the first line of defense against unwanted intrusions, and serve to prevent hackers who do not have the requisite information, e.g. the password, etc., from accessing the computer networks and systems. Secondly, the encryption and message authentication systems ensure that any information that is stored or in transit is not readable and cannot be modified. In the event that a hacker is able to break into the computer network, these systems prevent the information from being understood, and, as

such, encryption systems act as the second line of defense. Further, intrusion detection systems uncover patterns of hacker attacks and viruses and, when discovered provide an alarm to the system administrator so that appropriate action can be taken. Since detection systems operate only after a hacker has successfully penetrated a system, such systems act as a third line of defense.

Obviously, as an access control system is the first line of defense, it is important that the selection thereof be well-suited to the application. In access control systems there is a broad dichotomy between user authentication and host authentication systems. In current practice, the most common user authentication systems include simple password systems, random password systems, and biometric systems. The simple password systems are ubiquitous in our society with every credit card transaction using a pin identification number, every automatic teller machine inquiry looking toward a password for access, and even telephone answering messages using simple password systems for control. To this in random password systems another level of sophistication is added. In these systems, the password changes randomly every time a system is accessed. These systems are based on encryption or a password that changes randomly in a manner that is synchronized with an authorization server. The Secure ID card is an example of such a system. Random password systems require complimentary software and/or hardware at each computer authorized to use the network. In biometric systems, characteristics of the human body (such as

voice, fingerprints or retinal scan) are used to control access. These systems also require software and/or hardware at each computer which is authorized to use the network. The other category of access control is that of host authentication. Here the commonest systems are those of "call back" and "firewall" systems. Call back systems are those systems which work by calling a computer back at a predetermined telephone number. These systems authenticate the location of a computer and are suitable for dial-up (modem) networks; however, such systems are ineffective when the attack comes via the Internet. On the other hand, firewall systems are designed to prevent attacks coming from the Internet and work by allowing access only from computers within a network. Even though firewall systems are implemented either as standalone systems or incorporated into routers, a skilled hacker is still able to bypass such a host authentication system.

Currently, all the security products that perform access control are based on "in-band" authentication - i.e. the data and authentication information are on the same network. For example, upon accessing a computer, a computer prompt requests that you enter your password (authentication information) and, upon clearance, access is granted. In this example, all information exchanged is on the same network or may be termed "in-band." The technical problem which arises is that the hacker is then placed in a self-authenticating environment.

Except for callback systems, typically the access control

products authenticate only the user and not the location. At a time when computer networks could only be accessed by modems, the authentication of location by dialing back the computer which requested the access provided a modicum of security. Now as virtually all the computer networks are accessible by the Internet, which is modem independent, location authentication by callback is not secure. The lack of security arises as there is no necessary connection between the Internet address and a location, and, in fact, an Internet address most often changes from connection to connection. Thus, callback systems are rendered useless against attacks originating from the Internet.

In preparing for this application, a review of various patent resources was conducted. The review resulted in the inventor gaining familiarity with the following patents:

ITEM NO.	PAT. NO.	INVENTOR	ORIG. CLASS	ISSUE DATE
1	5,898,830	Wesinger ***et al.***	395/187.01	04/27/1999
2	5,680,458	Spelman ***et al.***	380/21	10/21/1997
3	5,615,277	Hoffman	382/115	03/25/1997
4	5,588,060	Aziz	380/30	12/24/1996
5	5,548,646	Aziz ***et al.***	380/23	08/20/1996

In general terms, the patents all show a portion of the authentication protocol conducted out-of-band. For purposes of this discussion an "out-of-band" operation is defined as one conducted without reference to the host computer or any database in the host network.

In Item 1, the patent to Wesinger ***et al.***, U.S. Patent

5,898,830 ('830) is a firewall patent. Here, the inventor attempts to enhance security by using out-of-band authentication. In his approach, a communication channel, or medium, other than the one over which the network communication takes place, is used to transmit or convey an access key. The key is transmitted from a remote location (e.g, using a pager or other transmission device) or and, using a hardware token, the key is to the conveyed local device. In the '830 system, to gain access, a hacker must have access to a device (e.g., a pager, a token etc.) used to receive the out-of-band information. Pager beep-back or similar authentication techniques may be especially advantageous in that, if a hacker attempts unauthorized access to a machine while the authorized user is in possession of the device, the user will be alerted by the device unexpectedly receiving the access key. The key is unique to each transmission, such that even if a hacker is able to obtain it, it cannot be used at other times or places or with respect to any other connection.

Next turning to Item 2, the patent to Spelman ***et al.***, U.S. Patent 5,680,458 ('458), a method of recovering from the compromise of a root key is shown. Here, following the distribution of a new replacement key, an out-of-band channel is used by a central authority to publish a verification code which can be used by customers to verify the authenticity of the emergency message. The '458 patent further indicates that the central authority uses the

root key to generate a digital signature which is appended to the emergency message to verify that the emergency message is legitimate.

Hoffman, U.S. Patent 5,615,277, is next discussed. Here, biometrics are combined with a tokenless security and the patent describes a method for preventing unauthorized access to one or more secured computer systems. The security system and method are principally based on a comparison of a unique biometric sample, such as a voice recording, which is gathered directly from the person of an unknown user with an authenticated unique biometric sample of the same type. The Hoffman technology is networked to act as a full or partial intermediary between a secured computer system and its authorized users. The security system and method further contemplate the use of personal codes to confirm identifications determined from biometric comparisons, and the use of one or more variants in the personal identification code for alerting authorities in the event of coerced access.

Items 4 and 5 have a common assignee, Sun Microsystems, Inc., and both concern encryption/decryption keys and key management.

The submission of the above list of documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application. None of

the above show the novel and unobvious features of the invention described hereinbelow.

SUMMARY

In general terms, the invention disclosed hereby includes in the embodiments thereof, a unique combination of user and host authentication. The security system of the present invention is out-of-band with respect to the host computer and is configured to intercept requests for access. The first step in controlling the incoming access flow is a user authentication provided in response to prompts for a user identification and password. After verification at the security system, the system operating in an out-of-band mode, uses telephone dialup for location authentication and user authentication via a password entered using a telephone keypad. In addition and optionally the system provides further authentication using a biometric system. When voice recognition is employed for the biometric component, the user speaks a given phrase which the system authenticates before permitting access. Upon granting of access, the user now for the first time enters the in-band operating field of the host computer.

OBJECT AND FEATURES OF THE INVENTION

It is an object of the present invention to provide a host computer with a cost effective, out-of-band security network

that combines high security and tokenless operation.

It is a further object of the present invention to provide a network to isolate the authentication protocol of a computer system from the access channel therefor.

It is yet another object of the present invention to provide a separate security network which acts conjunctively with or as an overlying sentry box to the existing security system provided by the host computer.

It is still yet another object of the present invention to provide an authentication using a biometric component, such as speech recognition, to limit access to specific individuals.

It is a feature of the present invention that the security network achieves high security without encryption and decryption.

It is another feature of the present invention to have a callback step that restricts authentication to a given instrument thereby enabling restriction to a fixed location.

It is yet another feature of the present invention to combine callback and speech recognition in an out-of-band security facility.

Other objects and features of the invention will become apparent upon review of the drawings and the detailed description which follow.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following drawings, the same parts in the various views are afforded the same reference designators.

FIG. 1 is a schematic diagram of the security system of the present invention as applied to the internet in which an external accessor in a wide area network seeks entry into a host system;

FIG. 2 is a schematic diagram of the apparatus required for the security system shown in FIG. 1;

FIG. 3 is a schematic diagram of the software program required for the security system shown in FIG. 1 in which various program modules are shown for corresponding functions of the system and each module is shown in relation to the control module thereof;

FIG. 4 is a detailed schematic diagram of the software program required for the line module of the security system shown in FIG. 3;

FIG. 5 is a detailed schematic diagram of the software program required for the speech module of the security system shown in FIG. 3;

FIG. 6 is a detailed schematic diagram of the software program required for the administration module of the security system shown in FIG. 3;

FIG. 7 is a detailed schematic diagram of the software program required for the client/server module of the security

system shown in FIG. 3;

FIG. 8 is a detailed schematic diagram of the software program required for the database module of the security system shown in FIG. 3;

FIG. 9A through 9E is a flow diagram of the software program required for the security system shown in FIG. 1; and,

FIG. 10 is a schematic diagram of a second embodiment of the security system of the present invention as applied to the intranet in which an internal accessor in a local area network seeks entry into a restricted portion of the host system.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The out-of-band security system networks for computer network applications is described in two embodiments. The first describes an application to a wide area network, such as the internet, wherein the person desiring access and the equipment used thereby are remote from the host computer. The second embodiment describes the application of the disclosed invention to a local area network wherein the person desiring access and the equipment used thereby are within the same network (referred to as the "corporate network") as the host computer. For purposes of this description the person desiring access and the equipment used thereby are referred collectively as the "accessor".

In Figure 1, a general overview of the first embodiment of the out-of-band security networks for computer network applications of this invention is shown and is referred to generally by the reference designator 20. Here the accessor is the computer equipment 22, including the central processing unit and the operating system thereof, and the person or user 24 whose voice is transmittable by the telephone 26 over telephone lines 28. The access network 30 is constructed in such a manner that, when user 24 requests access to a web page 32 located at a host computer or web server 34 through computer 22, the request-for-access is diverted by a router 36 internal to the corporate network 38 to an out-of-band security network 40. Authentication occurs in the out-of-band security network 40, which is described in detail below. This is in contradistinction to present authentication processes as the out-of-band security network 40 is isolated from the corporate network 38 and does not depend thereon for validating data. The first shows a biometric validation which, in this case, is in the form of voice recognition and is within voice network 42. While voice recognition is used herein, it is merely exemplary of many forms of recognizing or identifying an individual person. Others include, but are not limited to fingerprint identification, iris recognition; retina identification, palms recognition, and face recognition. Each of these are similar to the first embodiment in that these is a requirement for monitoring the particular parameter of the individual person; including the parameter to a mathematical

representation or algorithm therefore; retrieving a previously stored sample (biometric data), thereof from a database and comparing the stored sample with the input of the accessor.

Referring now to Figure 2 a block diagram is shown for the hardware required by the out-of-band security network for computer network applications of this invention. The request-for-access is forwarded from the router 36 of the corporate network to a data network interface 50 which, in turn, is constructed to transfer the request to a dedicated, security network computer 52 over a data bus 48. The computer 52 is adapted to include software programs, see ***infra***, for receiving the user identification and for validating the corresponding password, and is further adapted to obtain the user telephone number from lookup tables within database 54 through data bus 48. The computer 52 is equipped to telephone the user through a PBX interface 56 and voice bus 58. For voice recognition, a speech or biometric system 60 is provided to process requested speech phrases repeated by the user 24 which is verified within the security computer 52. Upon authentication, access is granted through the data network interface 50.

Referring now to Figures 3 through 8 the software architecture supporting the above functions is next described. The security computer 52, Figure 2, is structured to include various functional software modules, Figure 3, namely, a control module 62,

a line module 64, a speech module including a biometric for voice recognition 66, an administration module 68, a client/server module 70, and a database module 72. The software program of the control module 62 functions and interconnects with the other modules (line, speech, administration, client/server and database modules) to control the processing flow and the interfacing with the internal and external system components. As will be understood from the flow diagram description, ***infra***, the control module 62 software of the security computer 52 incorporates a finite state machine, a call state model, process monitors, and fail-over mechanisms. The software program of the line module 64 is structured to provide an interface with the telephone network. The software program of the speech module 66 is structured to perform processing functions such as, but not limited to, speech verification, text-to-speech conversion and announcements. The software program of the administration module 68 is structured to archive the records of each call made, to provide security and management functions, and to process any alarms generated. The software program of the client/server module 70 is structured to enable a host computer or a web server 34 to interface with the out-of-band security network 40. The software program of the database module 72 is comprised of the databases to support the security network 40 which in the present invention includes an audit database, a subscriber database, a speech database, an announcement database, and a system

database.

Referring now to Figure 4, the line module 64 is described in further detail. The analog telephone interface 74 is the equipment, such as voice bus 58 and PBX interface 56, that interfaces to an analog line. The analog telephone interface 74 is, in turn, controlled by software program of the analog line driver 76. Similarly, digital telephone interface 78 is the equipment, such as data bus 48 and PBX interface 56, that interfaces to a digital line (T1 or ISDN PRI). The digital telephone interface 78 is, in turn, controlled by the software program of the digital line driver 80. The software program of the telephony functions module 82 is structured to accommodate functions such as, ***Call Origination, Call Answer, Supervisory*** signaling, ***Call Progress*** signaling, ***Ring*** generation/detection, ***DTMF*** generation/detection, and line configuration.

In Figure 5 the speech module 66 architecture is detailed. The speech verification (SV) hardware 84, (part of speech system 60, Figure 2) consists of digital signal processors that utilize SV algorithms for verification of an accessor's spoken password. The speech verification hardware 84 is controlled by the software program of the SV hardware driver 86. The software program of the speech verification processing unit 88 provides an interface with control module 62 and is structured to respond to queries therefrom for verifying an accessor's spoken password. Also, the SV

processing unit 88 enables the enrollment of users with the speech password and the interaction of the speech database of database module 72. The text-to-speech (TTS) hardware 90 consists of digital signal processors that utilize TTS algorithms. The text-to-speech hardware 90 is controlled by the software program of the TTS hardware driver 92. The software program of the TTS processing unit 94 provides an interface with the control module 62 and, as required by the control module 62, converts text strings to synthesized speech. The announcement hardware 96 consists of digital signal processors that utilize speech algorithms to record and play announcements. The announcement hardware is controlled by the software program of the announcement hardware driver 98. The software program of the announcement processing unit 100 also provides an interface with control module 62; upon demands of the control module 62, supplies stored announcements; and interacts with the announcement database of database module 72.

In Figure 6, the software program of the administration module 68 is presented in more detail. As the administration module 68 interfaces with the control module 62, see ***supra***, a subprogram, namely, a control module interface 102 is constructed to manage the communication therebetween. The administration module 68 further includes software to provide an audit trail of all calls requesting access. This unit or audit log 104 creates records about each call, which records are stored in the audit database of the database

module 72. Any alarms caused as a result of errors, threshold crossing or system failures are processed by the software program of alarm module 106. For remote administration of the out-of-band security system 40 of this invention, the software program of the network interface 108 is provided, which software communicates with the corporate network 38 (via network adapters). Access to the out-of-band security system 40 for administrative purposes is controlled by security module 110. Similar to the network interface 108, the software program of the management module 112 provides for the remote management of the out-of-band security system 40 for configuration, status reporting, software upgrades and trouble-shooting purposes.

Referring now to Figure 7, the software program of the client/server module 70 that secures the host computer or web server or router 34 of the corporate network 38 through the out-of band security system 40 of this invention is shown in detail. Here, the client protocol module 114 provides the interfacing means for the host computer or web server 34 and communicates with the out-of band security system 40 using a proprietary protocol. Alternatively, standard protocols such as RADIUS and TACACS can be used. The server protocol module 116 interfaces with the control module 62 and manages the interaction with the client protocol module 114.

In Figure 8 a detailed schematic diagram is shown of the software program required for the database module 72 of the out-of-

band security system 40 of this invention. The database module 72 is the recordkeeping center, the lookup table repository, and the archival storehouse of the system. In the above description numerous relationships to this module have already been drawn. The database module 72 communicates through control module interface 118 to the control module 62. Two types of communications are channeled to and from the database module 72, namely, communicating data for use during operations through database access interface 120 and communicating data for maintenance and provisioning of the out-of-band security system through database provisioning interface 122. While the databases described herein are specifically related to the application of this embodiment to voice recognition the formation of specific databases, e.g. a different set of samples of biometric parameters or characteristics, is within the contemplation of the invention. The databases hereof are the audit database 124 for the call records; the subscriber database 126 for subscriber information; the speech database 128 for aid in verifying an accessor's spoken password; the announcements database 130 for announcements to be played to users during a call; and, system database 132 for system related information (e.g. configuration parameters).

In Figure 9A through 9E the flow diagram for the above software program operation is shown and is described hereinbelow. Thus, while the preceding in discussing the network architecture for the out-of-band security system 40 explains the access portion

of the program - the operations side - and the configuration and maintenance portion of the program - the provisioning side, the description which follows is of the software operation of the out-of-band security system 40 from the receipt of a request-to-access inquiry to a granting-of-access or denial-of-access result. The logic description that follows reflects the accessor's inputs and the programmed processes along the logical pathway from the receipt of a request-to-access inquiry to a granting-of-access or denial-of-access result. The pathway commences at the **REQUEST FOR ACCESS** block 150 whereby a request to enter the host computer or web server 34 is received from the user at the remote computer 22. The user requesting access to the host computer from the remote computer is immediately prompted to login at the **LOGIN SCREEN PRESENTED** block 152. While the login procedure here comprises the entry of the user identification and password and is requested by the host computer 34, such information request is optionally a function of the security computer 40. Upon entry of data by user at the **ENTRY OF ID AND PASSWORD** block 154 the information is passed to the security computer 40. As described in the software architecture review, ***supra***, the software pathway of the login data is first to client module 114 at **SEND LOGIN DATA TO CLIENT MODULE** block 156 and then successively to server module 116 at **SEND LOGIN DATA TO SERVER MODULE** block 158 and to control module 62 at **SEND LOGIN DATA TO CONTROL MODULE** block 160. In transmitting the login data from the

client module 114 to the server module a proprietary protocol is employed, which protocol includes encryption of the data using standard techniques. The verification process is continued at the control module 62 which next enters the subscriber database 126 and retrieves at **CONTROL MODULE QUERIES SUBSCRIBER DATABASE AND RETRIEVES PASSWORD ASSOCIATED WITH LOGIN ID** block 162 the password associated with the logged in identification. The control module 62 verifies at **CONTROL MODULE VERIFIES PASSWORD** block 164 that the password received from the remote computer 22 is the same as the password retrieved from the subscriber database 126. Upon verification, the control module 62 at **DOES THE PASSWORD MATCH?** block 166 sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the control module 62 at **DOES THE PASSWORD MATCH?** block 166 initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. Alternatively, the program offers the user an opportunity to retry whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing. The retry process may be limited to a specified number of times. The message that the verification has been achieved is transmitted along the software pathway substantially in the reverse manner as the login data transmission. From the control module 62, the verification is

first received by the server module 116 and at **SEND VERIFICATION FROM SERVER MODULE TO CLIENT MODULE** block 168 the verification message along with the information that the authentication is proceeding is transmitted to the client module 114. In transmitting these messages to the client module 114 from the server module a proprietary protocol is employed, which protocol includes decryption of the data, where required, using standard techniques. The client module 114 transmits at **SEND VERIFICATION FROM CLIENT MODULE TO HOST COMPUTER** block 170 the messages to the host computer 34. Finally, the host computer 34 transmits at **SEND VERIFICATION FROM HOST COMPUTER TO REMOTE COMPUTER** block 172 the message that the login verification is complete is sent to the remote computer 22 and prompts the person or user 24 to stand by for a telephonic callback.

Now with the control module 62 having verified the remote computer 22, the software program hereof is constructed to have the control module 62 at **CALLBACK INITIATED BY CONTROL MODULE** block 174 initiate out-of-band the call-back procedure to the user 24. The control module 62 queries the subscriber database 126 and retrieves therefrom the telephone number associated with the login identification. Based on the data retrieved from the subscriber database, the control module 62 instructs the line module 64 at **DIAL USER TELEPHONE NUMBER** block 176 to call user 24. Upon user 24 answering the telephone at **USER ANSWERS TELEPHONE** block 178, the

software pathway continues with the line module 64 relaying to the control module 62 at **CONTROL MODULE NOTIFIED BY LINE MODULE OF OFF-HOOK CONDITION** block 180 that the user's telephone is off-hook. The program is constructed so that the control module 62 then instructs the speech module 66 at **SPEECH MODULE INSTRUCTED BY CONTROL MODULE TO RETRIEVE PASSWORD** block 182 to retrieve (or generate) a DTMF password. To accomplish this, the speech module 66 now queries the announcement database 130 and at **PROMPT RETRIEVED BY SPEECH MODULE** block 184 retrieves the prompt to be played to the user 24. Alternatively, the password for the prompt is generated and synthesized by the text-to-speech system 90, 92 and 94 of the speech module 66. At **PROMPT PLAYED BY SPEECH MODULE TO USER** block 186, the user 24 is instructed to impress the DTMF password on the telephone keypad. The program progresses so that after the user 24 enters the DTMF password on the telephone keypad at **USER ENTERS DTMF PASSWORD** block 188, the line module 64 at **LINE MODULE TRANSMITS ENTRY TO CONTROL MODULE** block 190 notifies the control module 62 of the entry made by user 24. In a manner similar to the login password, ***supra***, the control module 62 queries the subscriber database and, at **CONTROL MODULE RETRIEVES DTMF PASSWORD** block 192, retrieves the password or the generated password associated with the subscriber. At **CONTROL MODULE VERIFIES DTMF PASSWORD** block 194, the control module 62 verifies that the password entered at the telephone keypad by the user matches the password retrieved from

the subscriber database. Upon verification, the control module 62 at **DOES THE DTMF PASSWORD MATCH?** block 196 sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the control module 62 at **DOES THE DTMF PASSWORD MATCH?** block 196 initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. As in the previous password verification and alternatively, the program offers the user an opportunity to retry. Whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing. As before, the retry process may be limited to a specified number of times.

Upon out-of-band callback verification being received, the biometric identification portion of the software program is initiated. In this present embodiment, while the biometric parameter that is monitored is speech, any of a number of parameters may be used. In this case, the control module 62 instructs the speech module 66 at **SPEECH MODULE RETRIEVES PROMPT FOR USER** block 198 to retrieve a prompt that for the purpose of later playing the prompt to the user and collecting the speech password. The speech module 66 queries the announcement database 130 and retrieves the prompt to be played to the user 24. Besides using a prepared prompt, as above, a prompt synthesized by the text-to-speech system 90, 92 and 94 is utilizable for this purpose.

The prompt for collecting the speech password is played to the user 24 at **PROMPT USER AND COLLECT SPEECH PASSWORD** block 200. The user 24, who has previously had his biometric sample namely the speech pattern, registered with the speech database 128, then voices the speech password at **USER VOICES SPEECH PASSWORD** block 202 and transmits the same over the telephone at the remote computer 22 to the security computer 40. Then, at **SPEECH MODULE RETRIEVES SPEECH PASSWORD ASSOCIATED WITH LOGIN ID** block 204, the software program for the speech module 66 is adapted to query the speech database 128 and to retrieve the speech password associated with the accessor's login identification. Through the application of biometric analysis, such as voice recognition technology, the speech or module 66 at **SPEECH MODULE VERIFIES SPEECH PASSWORD** block 206 verifies that the voiced speech password received from the user 24 has the same pattern as the speech password retrieved from database 128. Upon verification, the speech module 66 at **DOES THE SPEECH PASSWORD MATCH?** block 208 sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the speech module 66 at **DOES THE SPEECH PASSWORD MATCH?** block 208 notifies the control module 62 which initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. As in the previous password verification and alternatively, the program offers the user an opportunity to retry. Whereupon there is

a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing. As before, the retry process may be limited to a specified number of times. Upon being notified of a match between the pattern of the voiced speech password and that of the one retrieved from the database 128, the control module 62 at **CONTROL MODULE INSTRUCTS SPEECH MODULE TO ANNOUNCE ACCESS IS GRANTED** block 210 instructs the speech module 66 to provide an announcement to the user 24 indicating that access is granted. The speech module 66 queries the announcement database 130 and retrieves the announcement for the user 24. Alternatively, the announcement can be synthesized by the text-to-speech system 90, 92 and 94 and played to the user 24. Whichever announcement is used, it is made to the user at **ACCESS GRANTED ANNOUNCEMENT MADE TO USER** block 212.

Upon completion of the announcement at **SPEECH MODULE NOTIFIES CONTROL MODULE OF ANNOUNCEMENT** block 214, the speech module 66 notifies the control module 62 that the announcement has been made to the user 24. At this point at **DISCONNECT TELEPHONE CONNECTION WITH USER** block 215, the control module 62 instructs the line module 64 to terminate the telephone connection and the telephone connection between the security computer 40 and user 24 is severed. At **CONTROL MODULE SENDS AUTHENTICATION MESSAGE TO SERVER PROTOCOL MODULE** block 216, the message that user 24 is authenticated is

relayed by control module 62 to server protocol module 116 which is requested to communicate the same to the client protocol module 114. At **SERVER PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO CLIENT PROTOCOL MODULE** block 217, the message is relayed to the client protocol module 114 and thence via a proprietary protocol, at **CLIENT PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO HOST COMPUTER** block 218, to the host computer 34. The host computer or web server 34 at **HOST COMPUTER GRANTS ACCESS TO USER** block 219 grants access to the authenticated user 24.

In Figure 10 a schematic diagram of the second embodiment of the present invention is shown. For ease of comprehension, where similar components are used, reference designators "200" units higher are employed. In contrast to Figure 1 which describes the out-of-band security networks for computer networks of this invention as applied to the internet or wide area networks, this embodiment describes the application to local area networks. The second embodiment is referred to generally by the reference designator 220. Here the accessor is the computer equipment 222, including the central processing unit and the operating system thereof, and the person or user 224 whose voice is transmittable by the telephone 226 over telephone lines 228. While in this example the biometric parameter monitored is voice patterns as interpreted by voice recognition systems, any of a number of other parameters may be used to identify the person seeking access. The access

network 230 is constructed in such a manner that, when user 224 requests access to a high security database 232 located at a host computer 234 through computer 222, the request-for-access is diverted by a router 236 internal to the corporate network 238 to an out-of-band security network 240. Here the emphasis is upon right-to-know classifications within an organization rather than on avoiding entry by hackers. Thus, as the accessor is already within the system, the first level of verification of login identification and password at the host computer is the least significant and the authentication of the person seeking access is the most significant. Authentication occurs in the out-of-band security network 240, which is analogous to the one described in detail above, except the subscriber database becomes layered by virtue of the classification. This is in contradistinction to present authentication processes as the out-of-band security network 240 is isolated from the corporate network 238 and does not depend thereon for validating data. The overview shows the biometric validation which, in this case, takes the form of a voice network 242.

Because many varying and different embodiments may be made within the scope of the inventive concept herein taught, and because many modifications may be made in the embodiments herein detailed in accordance with the descriptive requirement of the law, it is to be understood that the details herein are to be interpreted as illustrative and not in a limiting sense.